CENSORSHIP AND SURVEILLANCE OF JOURNALISTS: AN UNSCRUPULOUS BUSINESS

REPORTERS
WITHOUT BORDERS
FOR FREEDOM OF INFORMATION

A REPORTERS WITHOUT BORDERS INVESTIGATION
REZA MOINI / BENJAMIN ISMAIL / ELODIE VIALLE

CONTENTS

Cover : FRED TANNEAU / AFP

INTRODUCTION

On World Day Against Cyber-Censorship, Reporters Without Borders (RSF) condemns the readiness with which leading Internet companies submit to the censorship demands of authoritarian regimes.

It also deplores the lack of international mechanisms regulating surveillance technology, which allows technology companies to sell online surveillance tools to these regimes even if it means trampling on human rights to increase their market share.

1 INTERNET GIANTS THAT TOLERATE OR ACTIVELY COOPERATE WITH CENSORSHIP

The New York Times revealed in November 2016 that, with owner Mark Zuckerberg's support, Facebook had secretly developed software to stop certain content from appearing in users' news feeds in specific geographic areas. Facebook sources told the newspaper that the software's aim was to satisfy the Chinese regime's censorship requirements. It was created to help the US social network giant get back into the Chinese market, from which it was expelled seven years ago during a period of unrest by the Uyghur minority in Xinjiang, which used Facebook to circulate information about the crackdown on protests and riots.

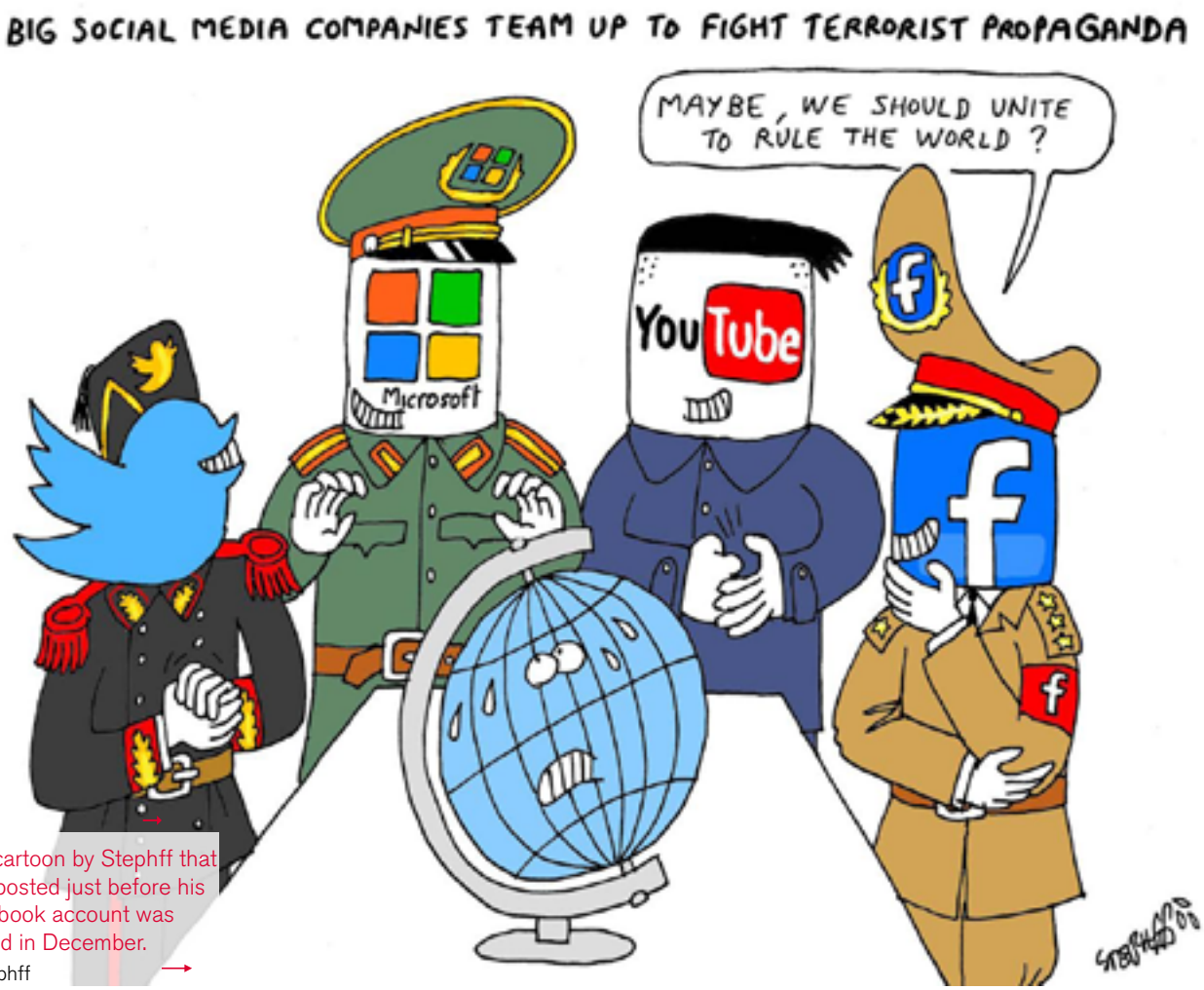
There is growing concern about Facebook's active cooperation with certain governments, its deletion of journalistic content and its opaque content "moderation" policies. The many examples include the blocking of the fan page of ARA News, a website that covers developments in Syria, Iraq, Turkey and other parts of the Middle East and claims to receive thousands of visitors a day on its Facebook page. The California-based company blocked the ARA News fan page for several days last December without any explanation.

Stephff, a Thai cartoonist known for his sarcastic drawings, found that his Facebook account had been suppressed shortly after he posted a cartoon on Facebook and other social networks. The Facebook account of David Thomson, a Radio France Internationale journalist who specializes in covering Jihad, was blocked in June 2016 on the grounds that an Islamic State flag could be seen in a photo. The journalist Kevin Sessums, and the famous 1972 photo of a Vietnamese girl who had just been burned in a napalm attack are among the many victims of Facebook's arbitrary censorship that have ended with the content or account being restored, the lifting of a ban and the same apology: "*We're very sorry about this mistake. The post was removed in error and restored as soon as we were able to investigate. Our team processes millions of reports each week, and we sometimes get things wrong.*"

> "WE SOMETIMES GET THINGS WRONG"

The examples of content arbitrarily censored by Facebook include this photo of a young Vietnamese girl burned by napalm.

©www.presse-citron.



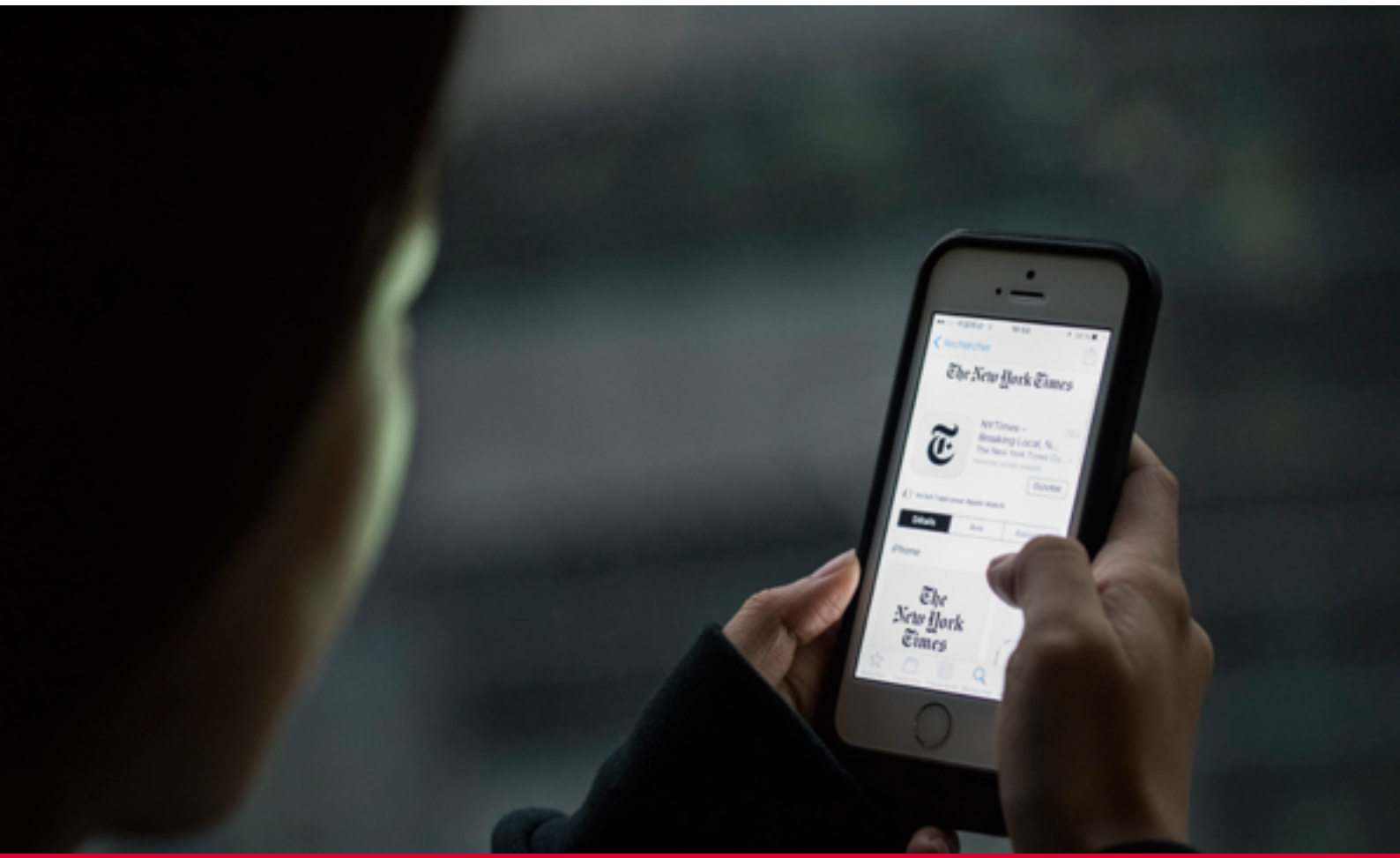
The cartoon by Stephff that was posted just before his Facebook account was closed in December.
©Stephff

The other Internet giants are not much better. Twitter was repeatedly accused of censoring journalists in 2016. In Turkey, Twitter used its local content management tool for blocking access to a tweet or an account from within a given country. On its website, Twitter says it only acts on "a valid and properly scoped request." But it quickly implemented the orders issued just a few days after Turkey's 15 July abortive coup, censoring more than 20 accounts of journalists and media outlets. Most of the censored accounts were those of former reporters and editors of the newspaper Zaman Amerika. They also included a Kurdish journalist, @AmedDicleeT, with 186,000 followers, the Kurdish daily Özgür Gündem (@ozgurgundemweb1) and even the official account of the Kurdish news agency DIHA (@DicleHaberAjans).

"We have challenged (at great expense on Twitter) many of the withholdings in Turkey in Court, including a majority of the verified accounts (of journalists). The content may remain visible until the appeal is resolved", answer Twitter.

Apple received criticism in January 2017 when the New York Times reported that both the English-language and Chinese-language versions of the NYT app had been removed from the iTunes store in China at the request of the Cyberspace Administration of China (CAC), the official body that monitors the Internet for the Communist Party. Self-censorship by iTunes had already been noted shortly after it created its first store in China in 2008. Apple has since blocked many apps about the Dalai Lama and other subjects that are taboo in China. In late 2015, a US businessman travelling from Hong Kong to Mainland China saw how the Apple News app was suddenly blocked . In September 2015, Apple blocked an app created by Josh Begley, a journalist with The Intercept, that monitors all drone strikes carried out by the United States, and an app about the shooting in Ferguson, Missouri.

Apple withdrew the New York Times app from its iTunes store in China. ↓



2 THE DUBIOUS BUT LUCRATIVE SURVEILLANCE BUSINESS

Surveillance of the Internet and telecommunications is above all the prerogative of governments that are on RSF's list of Enemies of the Internet, regimes that cite "the nation's vital interests" as grounds for being the most repressive in the world with regards to online freedom of information. The front runners are authoritarian regimes such as China, Iran, Syria and Uzbekistan, which have acquired and continue to acquire technology that allows them to spy on anything said or done by critical journalists, bloggers and Internet activists.

In countries that are regarded as democratic, such as France, the United Kingdom, United States, Australia and Mexico (see below), surveillance technology is used on security grounds and the confidentiality of journalists' sources is under attack.

Is an ethical role for telecom companies in Iran possible?

Iran is one of the most repressive countries with regards to monitoring and controlling Internet users. A cyber-police force keeps a permanent eye on the Iranian public's online activities. In the past three years, more than 100 Internet users, including many journalists and citizen journalists, have been arbitrarily summoned and arrested in various cities and some have been given harsh sentences.

Most of these journalists, both professional and non-professional, are the victims of surveillance technology known as Lawful Interception Management Systems (LIMS). But even under the Revolutionary Guard, this technology is used in an unlawful manner in Iran. In the wake of the historic accord on nuclear issues reached in January 2015, a growing number of telecom sector companies (including Vodafone, Telecom Italia, AT&T and Nokia) envisage investing in Iran. The French company Orange has begun talks on acquiring a stake in the leading Iranian mobile phone company MCI, which is controlled by the Revolutionary Guard, although it is vague about its intentions. "*Like other international operators, the group is studying the opportunities offered by the Iranian market*," Orange has said. Vivaction is another French company that is in "the phase of rediscovering the market" in Iran. Richard Marry, one of its representatives said: "*We have been going every month to Iran for more than 12 months to meet with the telecom ecosystem*."

Reza Moini, the head of RSF's Iran-Afghanistan desk, comments: *"With a mobile phone penetration rate of well over 100% and given that almost one household in two has a fixed line Internet connection, it is not only legitimate to ask what kind of presence international companies plan to establish in Iran but it is also essential that these companies are transparent about the accords they sign or are about to sign with the regime. We don't want a repetition of the Nokia-Siemens and Ericsson cases."*

RSF issued a statement in September 2011 criticizing the kind of cooperation that exists between many western companies and the Iranian regime and calling for international sanctions to be applied against them whenever it was established that the technology or infrastructure that they were installing in Iran allowed the regime to spy on and persecute the population.

Hacking Team and NSO: abetting Enemies of the Internet

In a special report on surveillance in March 2013, RSF for the first time spotlighted five "digital era mercenaries" – companies based in the United Kingdom, Germany, Italy, France and the United States whose products are used by repressive regimes to violate human rights and freedom of information. They included the Milan-based company Hacking Team, which sells "offensive" surveillance technology to Morocco and the United Arab Emirates that is used by their governments to spy on news websites and human rights activists.

HackingTeam was back in the news again in July 2015, when hackers got into its networks and obtained several hundred gigabytes of data, including many emails about its clients and the products being sold to them. The emails confirmed that France, Morocco, Sudan and Thailand and other countries were interested in its products, including Remote Control System (RCS), which was designed to enable government agencies to circumvent data encryption. The hacked emails also revealed that the Rwandan government had tried unsuccessfully to buy RCS in 2012. More surprisingly, they also showed that Mexico was HackingTeam's biggest client, with 6 million dollars of purchases. The list of Mexican clients included the interior ministry, the federal police, the army, the navy, the domestic intelligence agency, the attorney-general's office, state governments and even the state oil company PEMEX.

In response to the widespread adoption of governmental online surveillance in Mexico, the digital rights group Red en Defensa de los Derechos Digitales (R3D) brought a legal challenge on behalf of a group of journalists, human rights activists and students against a provision in the Federal Telecommunications Act that allows the authorities to retain large amounts of metadata without recourse to a judge. After Mexico's supreme court rejected the challenge on 11 May 2016, the coalition appealed to the Inter-American Court of Human Rights. Journalists, bloggers and cyber-activists meanwhile continue to be vulnerable to spying by their government, whose dealings with Hacking Team clearly show that it is bent on mass surveillance of the Internet and telecommunications.

"Rely on us" – an advertisement for Hacking Team, a company criticized for selling "offensive" surveillance technology.

©Capture d'écran du site d'HackingTeam. ↓

When questioned, the companies concerned – including Hacking Team in Italy – defended their activities by pointing to the need to combat terrorism and stating that they complied with the laws in the countries where they are based.

"This is not an adequate response, inasmuch as their technology continues to be used by authoritarian regimes that are Enemies of the Internet to spy on and imprison journalists," Christophe Deloire said.

"Given the commercial relations that exist between many Mexican governmental entities and one of the leading exporters of surveillance technology, you cannot help wondering about the ability of Mexico's journalists to do independent investigative reporting and protect their sources," said Emmanuel Colombié, the head of RSF's Latin America desk. *"The lack of transparency on the part of the authorities on the intended use of this technology reinforces our concern. There must be safeguards against its systematic use to target news providers, media professionals, bloggers and human rights activists."*

PEGASUS COULD OBTAIN CONTACTS, EMAILS, TEXT MESSAGES, THE DETAILS AND CONTENT OF CALLS, AND CONVERSATIONS ON WHATSAPP, SKYPE AND EVEN TELEGRAM, WHICH IS REPUTED TO BE SECURE.

Recent revelations suggest that the Mexican authorities used Pegasus, spyware developed by the Israeli company NSO, to spy on Rafael Cabrera, a Mexican investigative journalist working for various outlets including the Aristeguinoticias.com website. The existence of Pegasus was revealed in August 2016 by Citizen Lab and Lookout. By exploiting several iPhone security flaws (subsequently corrected), it could take complete control of the iPhone of any user who clicked on a malicious hypertext link sent by SMS. Pegasus could obtain contacts, emails, text messages, the details and content of calls, and conversations on WhatsApp, Skype and even Telegram, which is reputed to be secure. It could even remotely activate the phone's camera and microphone and trace the phone's location at any time.

"NSO helps make the world a safer place by providing authorized government agencies with technology that helps them combat terror and crime. Customers can use the product exclusively for the investigation and prevention of crime and terror. The ethical and lawful use of its product by the customers is of utmost importance to the company. In case of an alleged breach of the contract, the company will take appropriate action with the respective customer", affirmations that RSF was not able to verify.

Pegasus was used to spy on **Cabrera** after he contributed to the investigative reporting that exposed the so-called "Mexican White House" scandal implicating President Enrique Peña Nieto's family. According to the New York Times, the Mexican government paid 15 million dollars to NSO for three unspecified projects. Cabrera received several suspect messages asking him go to UNO TV's headquarters and "informing" him that the president was considering bringing a defamation prosecution against the journalists involved in the "White House" investigation in order to have them jailed.

Journalist Rafael Cabrera and the aristeguinoticias team, targets of the Pegasus spyware. →

NSO claimed that the software it sold was solely used for legal surveillance. But, at the time that these revelations were taking place, Citizen Lab exposed a similar surveillance attempt targeting **Ahmed Mansoor**, an Emirati blogger and administration of Al-Hera, a democracy discussion forum. Mansoor received the same SMS on his iPhone 6 twice, on 10 and 11 August 2016, with a link that would supposedly provide him with information about human rights abuses by the Emirati government. Citizen Lab's analysis of the SMS message established a connection to Pegasus and NSO.

3 INTERNATIONAL REGULATIONS: BROKEN OR BLOCKED BY LOBBIES

The resolution on the promotion, protection and enjoyment of human rights on the Internet, adopted by the UN Human Rights Council during its 32nd session (from 13 June to 1 July 2016), reiterated that: "*The same rights that people have offline must also be protected online, in particular freedom of expression, which is applicable regardless of frontiers and through any media of one's choice, in accordance with articles 19 of the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights.*" It also urged all states to "*address security concerns in accordance with their international human rights obligations, in particular with regard to freedom of expression, freedom of association and privacy.*"

> THE HUMAN RIGHTS COUNCIL'S RESOLUTIONS ARE NOT BINDING AND ARE NOT AN EFFECTIVE WAY TO RESTRAIN THOSE STATES THAT ARE THE WORST VIOLATORS OF INDIVIDUAL ONLINE FREEDOMS.

Another Human Rights Council resolution, adopted in September 2016, noted that, "*in the digital age, encryption and anonymity tools have become vital for many journalists to exercise freely their work and their enjoyment of human rights, in particular their rights to freedom of expression and to privacy, including to secure their communications and to protect the confidentiality of their sources*," and called on Member States "*not to interfere with the use of such technologies, with any restrictions thereon complying with States' obligations under international human rights law.*"
However, the Human Rights Council's resolutions are not binding and are not an effective way to restrain those states that are the worst violators of individual online freedoms.

Ever since Edward Snowden's revelations and the end of US hegemony over Internet governance, the Enemies of the Internet have been trying to increase their role in Internet regulation, above all via such UN agencies as the International Telecommunication Union, UNESCO and the United Nations Conference on Trade and Development, which have all issued declarations on the defence of fundamental freedoms online and Internet governance. Following the Declaration of Principles issued at the World Summit on the Information Society (WSIS) in Geneva in 2014, the WSIS has been one of the main multilateral platforms on Internet governance, but it has issued no binding resolutions designed to prevent authoritarian regimes from subjecting their citizens to mass censorship and surveillance.

"There is a growing danger that the struggle over the strategic issue of Internet governance will end up officialising a fragmented and censored Internet," said Benjamin Ismaïl, the head of RSF's Asia desk. *"If every country demands sovereignty over the Internet, we will have a system that grants authoritarian regimes every right to restrict online free speech and information. To avoid this, it is essential that binding international mechanisms are put in place to guarantee the existence of a global free Internet. Now more than ever, this guarantee requires control of Internet companies and companies that export mass surveillance technology."*

US National Security Agency (NSA) whistleblower Edward Snowden

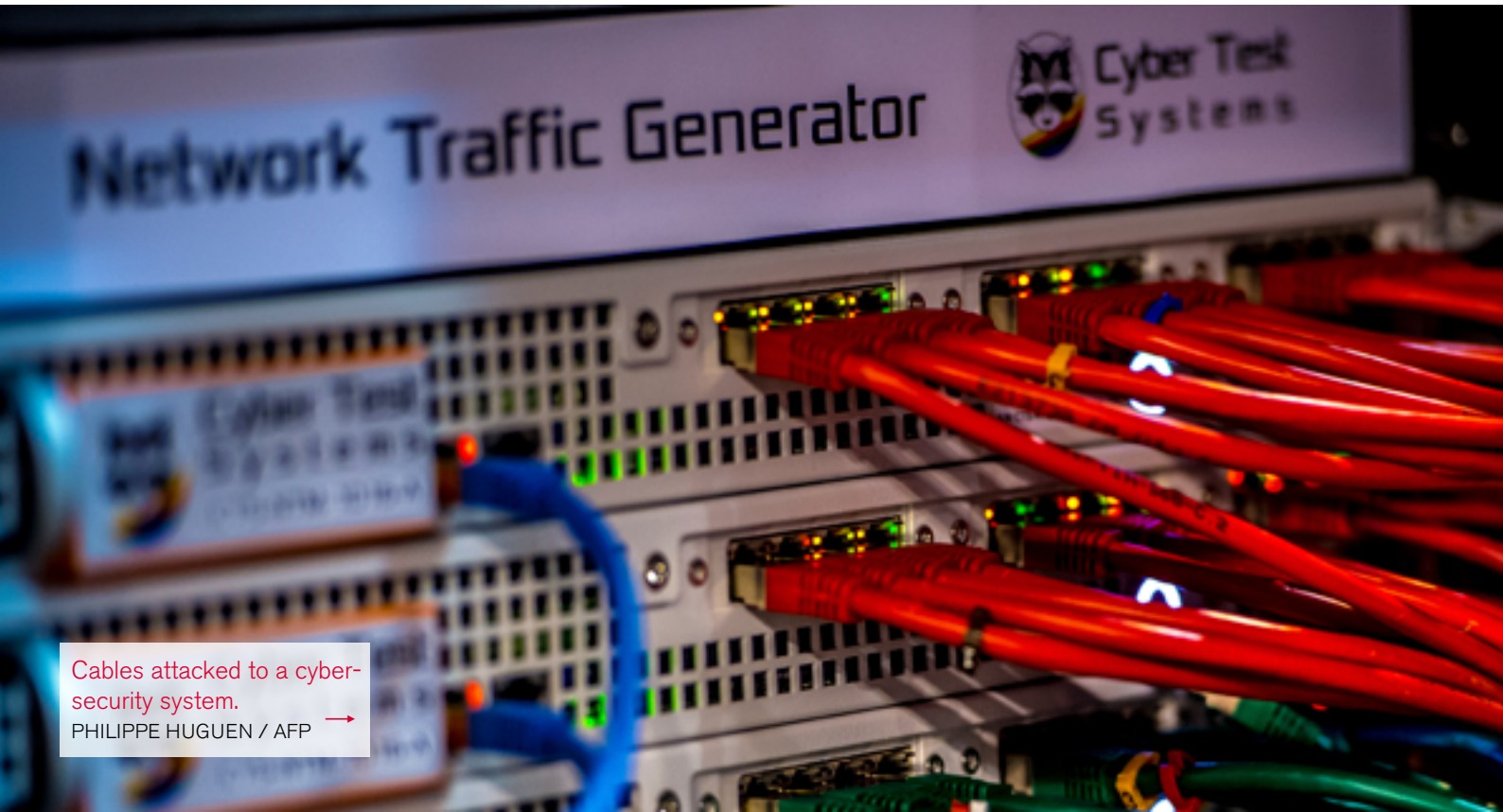
FREDERICK FLORIN / AFP

In June 2014, RSF began asking the UN Human Rights Council to establish an international convention on corporate responsibility with regard to human rights, with the aim of making governments place strict controls on the export of surveillance technology and establish effective recourse for individuals who have been the victims of surveillance and the terrible consequences that can result from it (arrest, imprisonment, physical violence and torture).

A few months later, on 28 November 2014, RSF, Privacy International, Digitale Gesellschaft, the International Federation for Human Rights (FIDH) and Human Rights Watch hailed the European Union's decision to add new forms of surveillance technology to the list of dual-use goods and technologies subject to export controls. It was "*Europe's first step towards increased control of surveillance technology*," RSF said. Members of the Coalition Against Unlawful Surveillance Exports (CAUSE) – Reporters Without Borders, Amnesty International, Digitale Gesellschaft, FIDH, Human Rights Watch, Open Technology Institute and Privacy International – sent a joint open letter on 2 December 2014 to members of the Wassenaar Arrangement, a grouping of 41 nations – most of them EU members – that regulates the export of conventional arms and dual-use goods and technologies. Referring to the Wassenaar Arrangement upcoming plenary session, the letter urged the groupe to take measures to curb the alarming proliferation of surveillance technology available to authoritarian regimes known to systematically violate human rights.

NEARLY THREE YEARS AFTER THESE CALLS FOR EFFECTIVE CONTROL OF THE PRIVATE SECTOR, THE EU APPEARS TO BE IN RETREAT.

Regulation of surveillance technology exports has ground to a halt as a result of pressure from the digital technology industry lobby. Represented above all by the DigitalEurope association, whose executive board includes representatives of such companies as Nokia, Siemens, AMETIC, IBM, ANITEC, Cisco and Microsoft, and backed by a group of diplomats from nine countries (Austria, Finland, France, Germany, Poland, Slovenia, Spain, Sweden and United Kingdom), this lobby has managed to get telecommunications interception equipment, intrusion software, surveillance centres and data storage systems removed from the initial list of technology subject to control in the regulation proposed by the European Parliament and Council.



Cables attacked to a cyber-security system.
PHILIPPE HUGUEN / AFP →

The latest proposal no longer contains the originally envisaged controls on biometric equipment, geolocation systems or deep packet inspection technology (DPI), which enables inspection of data packets as they move through the Internet. By using DPI, governments bent on surveillance can access the content of emails, instant messaging, and VoIP conversations, and can see whether or not an email or message is encrypted. The latest proposal also fails to obligate EU member states to tell the public which companies have been given permission to export.

Within the United Nations, the European Union and most national legislation, regulation of Internet surveillance, data protection and surveillance technology exports is still incomplete and inadequate with regard to international human rights norms and standards. The need for a legislative framework that protects online freedoms continues to be primordial with regard to both the issue of Internet surveillance as a whole and the particular problem of companies that export surveillance technology.

4 RSF's recommendations on cyber-censorship

To combat cyber-censorship, Reporters Without Borders (RSF) asks:

Private-sector companies:

- To improve their transparency reports and publish them systematically, and to publish the official requests they receive from governments to withdraw content or delete user accounts.
- To respect the Universal Declaration of Human Rights and UN human rights conventions.
- To respect the UN's Guiding Principles on Business and Human Rights and develop precise plans to implement them.
- To adopt codes of ethics and effective traceability mechanisms for the technology they export.
- To ban the export of surveillance technology to non-democratic and authoritarian countries and to accept that they have a duty to be vigilant and to identify threats to – and prevent serious violations of – human rights, fundamental freedoms and person security.
- To apply the principles of "responsible contracts" developed by John Ruggie, the UN Secretary-General's Special Representative for Human Rights and Transnational Corporations and other Business Enterprises, under which companies are held partly responsible for the serious human rights violations that could result from their technology.

Governments:

- To treat unrestricted Internet access and guaranteed digital freedoms as fundamental rights.
- To adopt laws guaranteeing digital freedoms, including the protection of privacy and personal data from intrusion by the police or intelligence services, and establish appropriate appeal mechanisms.
- To ensure that communications surveillance measures adhere strictly to the principles of legality, need and proportionality, in accordance with article 19 of the International Covenant on Civil and Political Rights.
- To be more open and transparent about surveillance requests submitted to companies, including the number of requests, their legal basis and their purpose.
- To bring their policies into line with those of the governments that best control technology exports and sanction companies that cooperate with authoritarian regimes.

The European Union:

- To add unrestricted Internet access and guaranteed digital freedoms to the Charter of Fundamental Rights of the European Union.
- In relations between EU members, with other countries and with international bodies such as the WTO, to treat Internet surveillance mechanisms as protectionist mechanisms and barriers to trade, and combat them as such.
- To ensure that there are standardized and uniform procedures for monitoring and controlling surveillance technology and for sanctioning its misuse.

The United Nations:

- To reinforce the mandate of the UN Working Group on the issue of Human Rights and Transnational Corporations and other Business Enterprises, in particular, by allowing it to receive individual complaints and to investigate individual cases of human rights violations linked to businesses.
- To consider drafting an international convention on Internet surveillance technology exports under which the exportation of this technology could be controlled and could be banned in the case of a substantial riskthat it could be used to commit or facilitate human rights violations.

5 JOURNALISTS: PROTECT YOUR DATA AND COMMUNICATION

To combat surveillance and censorship effectively, both professional and non-professional journalists should use software developed by civil society organizations and should take the concrete measures recommended in the guides to online security that are available online. RSF's Safety Guide for Journalists, which was updated in 2015, contains many practical tips for staying safe online.

The advice provided below, which applies to both computers and smartphones, does not claim to be exhaustive. RSF often organizes cyber-security seminars and provides free tutorials.

Attention: Always research the tools you are going to use and the techniques you are going to adopt. Technology is evolving fast and today's good advice may no longer be good tomorrow

Journalists follow the Chinese Communist Party's national congress.
AFP PHOTO / Greg BAKER →

General online behaviour:

Before beginning to secure your computer and install software capable of encrypting communications and data, you should adopt good digital hygiene by following common sense advice that will help prevent anyone from hacking into your computer or email account.

Avoid prying eyes:.

- Don't work with your back to a window.
- When travelling by train or plane, put a privacy filter over your laptop screen. A privacy filter is a transparent sheet that blocks lateral vision so that only the person sitting directly in front of the screen (you) can see what's on it.
- As far as possible, avoid being separated from your equipment when travelling so that no one can remove files from your computer or install a Trojan horse on it.
- All operating systems (Windows, Mac OS and Linux) allow you to set a password to prevent easy access by others. Use this basic protection.
- Don't download any files or click on any links sent to you from unknown sources.
- Carefully check the email address or Twitter account of anyone who shares a link with you. If in doubt, verify the sender with other contacts or by using a search engine.
- If a file or sender seem suspicious to you, contact experts who can help you. The ever-helpful Citizen Lab analyses suspicious links and malware that have been received by dissidents and activists.

As well as taking the above precautions, do the following:

- Use antivirus AND anti-malware software such as Malwarebytes.
- Activate your firewall.
- Keep your operating system (Windows, Mac OS X, etc.) up to date.
- Encrypt your computer's data storage (a function included in OS X).

Digital tracks:

If you work in an Internet café or on a computer that is not your own, don't leave any traces of your work session when it is over:

- If you check your email, Facebook account or Twitter account, remember to disconnect afterwards.
- Erase your browsing history. It contains a lot of information that an expert could use to access your online accounts.
- Never save a password in the browser of a public computer. If you have saved one by mistake, erase the browsing history when you finish working.
- Delete form field content.
- Delete cookies.

The ways to delete this data varies from browser to browser. A good way to avoid making any mistakes is to use the private browsing mode in Firefox or Chrome.

Messaging and accessing online services:

Most online services (such as Twitter, Facebook, WordPress, Tumblr and Skype) allow you to recover a lost password by emailing you a new one. It is therefore vital to protect your email account as much as possible. If it is compromised, your entire digital identity could be in danger.

Google's email service, Gmail, allows you to provide your account with an extra level of security by using two-step authentication. Once installed, your email account is protected by:

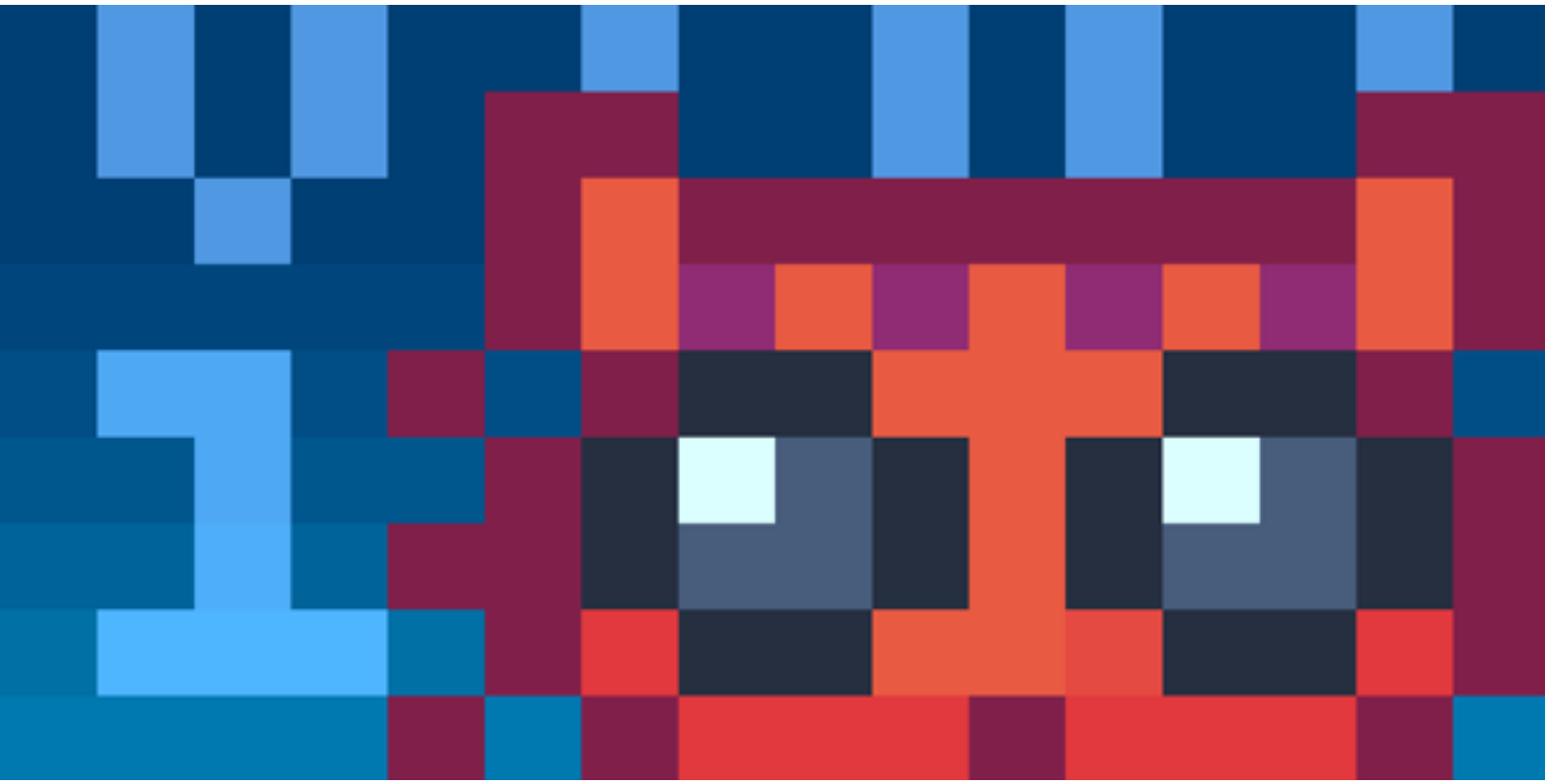
1. A username
2. A password
3. A different code that is sent to your mobile phone every time you want to connect to your inbox.

So, without your mobile phone, it is impossible to access your emails.

When you connect to your Gmail inbox, click on the "Details" link on the lower right of the page. This opens a window that shows all recent connections to you account and will allow you to see if there has been any suspicious activity.

You should also encrypt your emails and chats. As there are easy-to-use encryption tools, you should encourage your sources to use them so that all communications between you can be encrypted. They include:

- Cryptocat installs easily on a computer. Chats with fellow Cryptocat users are encrypted from end to end.
- Privnote and Zerobin are websites that allow you to create an online message that self-destructs as soon as it is read by the sole person to whom you can send a link to the message.
- Do you want to phone your sources via the Internet? No problem, but use Jitsi Meet, the "open-source Skype".



The logo of Cryptocat, a browser extension that encrypts chats and destroys them when they are over. ↑

Passwords:

Strong passwords need to be long. Length is the leading factor in a password's strength. So instead of passwords (which should be banned), we should refer to "pass phrases." They are the only way to resist a "brute force attack." And follow these tips:

- When creating a pass phrase, use digits and letters in uppercase and lowercase to create a sequence of characters that is relatively complex but at the same time easier to remember than a more abstract sequence of digits and special characters.

- Use a different pass phrase for each online service.

- Use a "password manager" such as LastPass, which is available as an extension for Firefox, Chrome and Safari. You can use it to safely store all your pass phrases.

Social network footprints:

Facebook and Twitter are very effective ways to communicate. But you should be careful about what information you are making available to the public. These tutorials and online services will help you monitor and control your online presence:

- Verify you Internet presence with "namechechk".

- Secure your Twitter account.

- Protect your privacy on Facebook when sharing content.

Secure browsing:

Use the following apps and plugins for Firefox and Chrome:

- https Everywhere: It makes websites use an encrypted HTTPS connection if available on the site and helps evade certain kinds of phishing.

- NoScript: It prevents (potentially dangerous) JavaScript scripts from executing on any website except those "whitelisted" by the user.

- Privacy Badger: It blocks the tracking cookies used by websites.

- Certificate Patrol: It verifies the certificates of HTTPs websites.

- A Virtual Private Network (VPN): It encrypts your Internet connections.

- Tor Browser: It allows you to browse anonymously.

Mobile phones:

- **Create and use** a code to communicate with your sources and other contacts. “Beep” them (by calling and letting their phone ring once or twice before hanging up) to let them know, for example, that you have arrived at a given location or that everything is all right.

- **Don’t put your contacts’ real names** in your phone’s contacts list. Assign them numbers or pseudonyms so that the police cannot get the details of your network of contacts if they ever seize your phone or SIM card.

- **Take a spare SIM card** with you to demonstrations if you think your SIM card might be confiscated. It is important to have a working mobile phone with you at all times. If you ever have to get rid of your SIM card, try to destroy it physically.

- **Lock your phone with a PIN** if it has this feature. All SIM cards have a default PIN. Change it and lock the card with this code. You will have to enter the phone PIN every time you use the phone.

- If you are at a demonstration and think the police may use force to disperse it, **turn on your phone’s flight mode**. You will no longer be able to make or receive calls, but you will still be able to take photos and shoot video, and upload them to websites later. This tactic is also useful if you think the police may target people at the demonstration who have phones. The authorities could later demand the call or SMS records or phone data of any individual at a given location at a given time in order to carry out mass arrests.

- **Turn off geolocation** in your apps unless you are using it to tag certain media outlets during an event for activism purposes. If you are using your mobile phone to live stream video, turn off the GPS and geolocation functions.

- If your phone uses the Android operating system, **software for encrypting your browsing, chats, texts and voice messages** is available from the Guardian Project and Open Whisper Systems. When using your phone to go online, use https whenever possible.

Combating censorship:

Some of the software listed above (such as VPNs and tools for anonymous browsing) also helps you to circumvent government censorship. For more information:

- Check out RSF's "Collateral Freedom" website. To help the citizens of certain countries circumvent website blocking by governments that violate human rights, RSF has used the technique of "mirroring" to create duplicates of the censored sites and put them on the servers of Internet giants such as Amazon, Microsoft and Google (which these governments would be reluctant to block).

- Visit the "Circumvention Central" website created by GreatFire (the NGO behind the "Collateral Freedom" initiative) to learn more about VPNs.

- Check out the Tactical Technology Collective's Security in-a-box website and these articles by the Electronic Frontier Foundation in order to be better able to circumvent online censorship and stay anonymous while online.

Launched in 2011, "Operation Collateral Freedom" makes it possible to access censored websites.. →

©RSF

REPORTERS WITHOUT BORDERS promotes and defends the freedom to inform and be informed throughout the world. based in paris, it has ten international bureaux (berlin, brussels, geneva, helsinki, madrid, stockholm, tunis, vienna and washington dc, Rio) and more than 150 correspondents in all five continents.

Secretary General: CHRISTOPHE DELOIRE
RSF editor-in-chief: VIRGINIE DANGLES

International Secretariat
CS 90247
75083 Paris Cedex 02
Tel. +33 1 44 83 84 84
Web : www.rsf.org

REPORTERS
WITHOUT BORDERS
FOR FREEDOM OF INFORMATION